REMARKS

In the Office Action, the Examiner rejected Claims 1-18, which are all of the then pending claims, as being unpatentable under 35 U.S.C. 103 over the prior art. Specifically, Claims 1, 3-5 and 7-18 were rejected as being unpatentable over International Application WO 01/595545 (Subramaniam) and U.S. Patent 5,870,473 (Boesch, et al.) and further in view of International Application WO 00/01108 (McLaughlin) and U.S. Patent 6,473,508 (Young, et al.). Claim 2 was rejected under 35 U.S.C. 103 as being unpatentable over Subramaniam and Boesch and further in view of McLaughlin; and Claim 6 was rejected as being unpatentable over Subramaniam and Boesch, et al. and further in view of U.S. Patent 5,794,207 (Walker, et al.).

The rejections of the claims are respectfully traversed. Also, independent Claims 1, 13 and 17 are being amended to better define the subject matters of these claims, and new Claim 19, which is dependent from Claim 1, is being added to describe preferred or optional features of this invention.

The rejections of the claims are respectfully traversed because the prior art does not disclose or suggest using two public/private key pairs together to establish a dialogue session, in which a trusted party is able to verify the source of messages, as described in the independent Claims 1, 13 and 17. The Examiner is, thus, requested to reconsider and to withdraw the above-identified rejections of Claims 1-18, and to allow these claims and new Claim 19.

In order to best understand this feature of the invention, and it significance, it may be helpful to review briefly the present invention and the prior art.

The present invention, generally, provides a method and system for parties to communicate in a dialogue over a computer network. One problem with many existing computer network dialogues, such as "chat rooms," is that there is no assurance that what is said is accurate or reliable. As a result, these dialogues are not suitable for many types of conversations such as business negotiations.

The present invention effectively addresses this issue and, in contrast to these prior art approaches, provides accountability for what is said during the dialogue. Generally, in accordance with the preferred embodiment of the invention, a plurality of users registers with a trusted body and then, through that trusted body, engage in a dialogue. The invention thus involves two parts – a registration process and a dialogue process.

As part of the registration process, each user generates a public/private key pair for a specific dialogue session and sends the public key of that pair to the trusted body. That trusted body verifies the identity of each user by using the public key sent to the trusted body. Once the identity of a user is verified, the trusted body generates a random identifier for the user and keeps a confidential record of the relation between the identity of each user and the random identifier for that user.

In the dialogue process, n one of the users enters into a dialogue with one or more other users by sending messages over the computer network and through the trusted body to said one or more other users. Each user is able to remain anonymous through use of its random identifier until such time as the user reveals it's identify to one or more of the other users. In addition, each message of the dialogue is encrypted using a public key of a second private key/public key pair of the trusted body, and the trusted body records these encrypted messages. The trusted body then uses the recorded dialogue, together with the confidential

record of the relation between the identity of a user and the random identifier, to provide a means to verify the dialogue by the users. Specifically, a user cannot effectively deny that he or she sent a particular message because all messages are sent through the trusted body, and that body records all those messages.

The prior art does not disclose or suggest the use of two private/public key pairs to establish a dialogue among users, as described above.

For example, Subramaniam describes a method and system for providing anonymous Internet transactions. In this method, an agent monitors and maintains the anonymity of transactions between two registered users on a secure computer system. After a user registers an account, the secure system permits the user to view and to post messages on the system. Each message posted to the system passes through the agent to prevent the inadvertent disclosure of identifying information by warning the user of the disclosure and requiring the user to authorize the disclosure before posting the message. Also, in the system disclosed in Subramaniam, each party may instruct the agent to permit the disclosure of identifying information.

Boesch, et al. describes a procedure for conducting economic transactions in a secure manner over insecure networks such as the Internet. Boesch, et al. is thus directed to security, not to verifying what was said between the parties. The Examiner cited Boesch, et al. for its discloser of generating a user identifier that is a random number. The procedure described in Boesch, et al. does not need to encrypt each received message, and clearly does not use the public key of a private/public key pair to do this.

There are a number of important differences between the present invention and the method and system disclosed in the combination of Subramaniam and Boesch, et al. It is

believed that the Examiner has recognized this, and thus has relied on McLaughlin and Young, et al. to reject the main Claims 1, 7 and 13.

McLaughlin discloses a procedure for processing bi-directional, anonymous or pseudo-anonymous user transactions. In this procedure, a number of digital certificates are created, and a plurality of operating modules is provided to perform various tasks. In normal operation, no one module within the system possesses enough information to determine the user's confidential identity and to connect the user to a particular transaction or to a particular anonymous or pseudo-anonymous identity.

Young, et al. discloses a digital signature infrastructure, and in particular, a public key that can be used to verify digital signatures but cannot be used to encrypt data in a way that prevents escrow authorities from decrypting the data.

In the Office Action, the Examiner specifically cited column 9, lines 21-35 of Young, et al. This portion of Young, et al. describes a key cryptosystem used for digital signatures. In this system, a user generates a public/private key pair and gives the public key to a Certificate Authority (CA). A sender signs a message using the sender's own private key, and the sender sends the message along with the signature to the receiver. The receiver obtains the message and signature, and obtains the public key of the sender from the CA. The receiver then verifies the authenticity of the received message using the message, the signature and the sender's public key.

There is a very important difference between this cryptosystem and the procedure of the present invention. Specifically, as described in Young, the sender signs the message using the sender's private key. In contrast, with this invention, the sender encrypts the message using the trusted body's public key.

The other references of record have been reviewed, and these other references, whether considered individually or in combination, also do not disclose or suggest the way in which the two public/private key pairs are used in the present invention to register the users and then conduct the dialogue.

For instance, Walker was cited by the Examiner for its disclosure of time stamping messages of a dialogue. This reference describes a buyer-seller protocol; in which a trusted third party may be used to determine fulfillment, adequacy and interpretation of a contract or contract offer.

Independent Claims 1, 13 and 17 describe the above-discussed feature of using two private/public key pairs. In particular, each of these claims describes the feature that each user registers with the trusted body by generating a first public/private key pair for a specific dialogue session, and sends the public key of that key pair to the trusted body. Each of Claims 1, 13 and 17 describes the further feature that the trusted body has a second public/private key pair, and that user encrypts each message of the dialogue using the public key of this second public key pair of the trusted body, and sends that encrypted message to the trusted body.

Because of the above-discussed differences between Claims 1, 13 and 17 and the prior art, and because of the advantages associated with those differences, Claims 1, 13 and 17 patentably distinguish over the prior art and are allowable. Claims 2-12, 18 and 19 are dependent from Claim 1 and are allowable therewith. Also, Claims 14-16 are dependent from, and are allowable with, Claim 13.

In view of the foregoing, the Examiner is respectfully requested to reconsider and to withdraw the rejections of Claims 1-18 under 35 U.S.C. 103, and to allow these claims and new Claim 19. If the Examiner believes that a telephone conference with Applicants' Attorneys would be advantageous to the disposition of this case, the Examiner is requested to telephone the undersigned.

Respectfully submitted,

John S. Sensny

John S. Sensny
Registration No. 28,757
Attorney for Applicant

Scully, Scott, Murphy & Presser, P.C.
400 Garden City Plaza - Suite 300
Garden City, New York 11530
(516) 7472-4343

LP:jy